

安全技术 in 计算机软件开发中的应用

夏永贞

(中国航空工业集团公司洛阳电光设备研究所,河南 洛阳 471000)

摘要:随着新时期发展,为了全面加强计算机软件开发水平,在开发计算机软件过程,技术人员要深入工作实际,结合安全技术管理内容,全面的构建更加完善的计算机软件开发体系,从而通过加强安全技术的应用,有效的保证计算机软件开发后的安全使用水平。通过实践分析,结合计算机软件开发工作实际,全面探索了安全技术 in 计算机软件开发中的应用策略。

关键词:计算机;安全技术;开发

【DOI】10.12231/j.issn.1000-8772.2022.06.157

1 引言

在计算机软件开发过程,有效的应用安全技术是必要的,作为技术人员,要提高安全技术研究能力,应在计算机软件开发中全面地进行安全技术应用分析,总结更加高效的的安全管理体系,从而全面提高计算机软件开发质量,进一步为计算机软件的开发与应用提供技术保证,具体分析如下。

2 计算机软件开发和安全技术介绍

2.1 软件开发

系统软件和应用软件都属于计算机软件的基本范畴,在实施软件开发的整个过程中有着重要作用。第一,进行开发的时候,可以利用系统软件和应用软件,从而让使用人员能够管理并维护好计算机。第二,利用开发软件来解决应用时候遇到的安全问题。第三,软件开发的工作环节,主要的特征就是体现是复杂性,而且还具有良好的应用价值。第四,不同行业中,计算机的应用都比较广泛,在应用多元化的基础上,必须要确保软件能够及时更新,从而充分体现应用的具体价值,全面提高了企业的社会效益以及经济效益。第五,实施软件开发这项工作,还要在人员和资金方面加大投入力度,并且开发环节由于复杂化还可能产生不良性影响,致使软件出现安全方面的问题。所以,一定要在开发环节把安全技术工作重视起来,以此确保软件开发工作的整体质量。

2.2 安全技术

随着社会经济的迅速发展,在计算机方面人们有了比以往要高的需求,不只是打字绘图那样简单的应用,而且主要还呈现出较为依赖的一种状态。平时生活和工作时,计算机功能的强大给各行各业的发展都带来了不同程度的助益,随之而来的还有安全隐患的频繁出现。比如,在软件编码过程,常有安全问题的出现,这些对于人们的日后的软件运用和工作都有不同程度的影响。因此进行软件开发工作的时候,必须要将应用安全技术的环节全面重视起来,以此采取安全防护的有效策略,全面提

高计算机软件的安全。

3 计算机软件开发环节常见的安全问题

3.1 软件编码漏洞和外部设施问题

整体而言,计算机软件在开发的过程当中,步骤处于比较复杂化的状态,软件编码时可能会有各种各样的漏洞出现,致使软件应用功能受到限制而发生安全问题。第一,安全问题限制了开发人员的技术水平,还制约着开发的条件,也让软件开发与软件设计的安全难以得到很好的保证。第二,关于软件应用网络环境复杂的问题,会有多样化的安全风险存在着,需要负责软件的开发人员能够在安全技术,软件防护方面不断加强,以此让各类安全风险能够得到有效性的应对。第三,软件应用的具体工作环节,还受到不同因素的影响,比如硬件设施和通信设备的影响等。如果外部环境因素致使设备故障,或者是线路老化,计算机应用时也会受到安全方面的威胁,从而影响着系统的稳定性运行。如果是比较严重的情况下,还会产生设备受损,系统崩溃的问题,为使用人员带来不同程度的损失。

3.2 管理问题

计算机软件在实际应用的时候,在数据加工,数据处理中可能会遇到外部的攻击,在用户传输信息中同样也会有安全问题出现,致使信息出现泄露的问题,严重的还可能会丢失。第一,信息管理的整个过程中,安全问题的产生主要分为主动攻击的形式和被动攻击的形式。第二,主动攻击是截取用户传输的信息内容,或是篡改使用人员的传输内容,致使信息结构被严重化的破坏。第三,在传输信息过程没有损坏的情况下入侵,采用窃听,监视的方法获得用户的数据信息,不仅攻击形式隐蔽,而且不容易被发现,这种属于被动攻击的形式。所以负责软件开发的工作人员,开发软件一定要利用好安全性的专业技术,从而全面提高软件的安全,同时也提高信息管理的核心能力,让风险在最大程度上得到减少。

3.3 遭受攻击

进行计算机软件应用中,可能经常会受到黑客、病毒的多方面攻击,威胁着计算机的整体性安全,因此要注意以下几个方面的内容。第一,黑客计算机应用的水平比较高,可以分析出计算机中存在的安全问题,并采取计算机技术展开对计算机的攻击,导致计算机系统问题,制约着软件开发的整体进程。第二,随着网络应用的不断发展,必要性的安全策略尤为重要,可以预防黑客的入侵,有效避免了计算机系统被破坏的情况,也有效避免了信息数据丢失情况的发生。第三,计算机应用常见的就是病毒攻击,具有很强的破坏能力。计算机受到攻击的时候还会涉及到系统的每个地方,出现很多程序无法正常运行的问题,进而也带来了严重的损失。可见软件开发的工作环节要进一步加强重视,并应用好安全技术。

4 计算机软件开发环节安全技术的应用

关于计算安全技术,在社会的发展下显得越来越重要了,因为安全可以让计算机内部存储或是重要性的信息得到良好的保护。具体而言,主要是要在计算机系统上开展信息系统硬件的保护,软件和内部数据的保护工作。而在安全技术当中,比较突出的工作内容就是计算内部软件的保护不受攻击,从而确保计算机信息不被泄露出去,同时也确保了计算机系统的安全性运行。

4.1 编码扫描以及编码加密技术

建立在内网与外网之间的通讯保护屏障,这个屏障就是防火墙技术,该技术是为了隔绝不安全的网络信息,进而营造网络环境的安全。第一,在实际应用的时候,内部所有网络的访问与连接,其数据都要通过防火墙的安全性监测,唯有数据确认合法合格才能够访问网络,有效预防了木马病毒、网络黑客的恶意性攻击,从而为开发软件提供了良好的环境。第二,防火墙是数据屏障,可以依据需要科学化,合理化的划分内部网络基本功能,并隔离内部主要网段,进而将网络运行影响运作的问题降低。

从漏洞扫描来分析,这项技术是在系统被攻击前实施的自我检查,同信息加密和防火墙技术相比较而言,呈现出来的主要特点就是自主化,也就是在没有被攻击以前利用漏洞检测技术,可以将网络中的问题检测出来,包括运作系统的检查,防火墙的检查等,从而在早发现中有效降低问题发生几率,确保企业效益的增强。

以符号作为基础,实施数据移位和数据置换算法的技术就是加密技术,该技术在软件开发的时候,由软件开发的工作人员利用对称加密能让非对称加密的技术重新编码目标信息,进而隐藏真正的信息内容,并促使不法分子无法获得真实信息内容,全面提高了信息系统的安全与可靠,同时也让的信息安全得到整体性提高。

4.1.1 密钥的应用和管理

密钥是信息加密技术的核心所在,也是保密与窃密的重点内容。第一,密钥有其自身的特点下,主要体现在私密和公开两个方面。但在信息交换的时候,涉及到的密

钥数量其实有很多,若是私密的密钥被第三方用户获得,信息交流过程就会被取代,从而也让用户的信息安全受到不同程度的威胁。第二,相同的密钥使用的次数如果过多,加密信息被泄露的风险就会增高。所以密钥使用的时候,负责技术的工作人员要更换处理好密钥,有效减少密钥被暴露的可能,并且还要确保密钥在应用时的安全。第三,技术人员可以在互联网中建立稳定化的密钥分配中心,利用这样的形式加以应用,一方面充分满足用户信息保密的实际需要,另一方面还能降低密钥重复使用的几率,切实地提高了整体安全性能。

4.1.2 量子加密技术的应用

在科学技术的日益发展下,作为新型加密技术,量子加密技术得到了合理化的应用,可以判断出信息是否被攻击,并且能实现全光网络,还能对密钥交换和信息加密级别加以提高。发现非法入侵者试图检测并接收用户需要的信息时,会影响到用户量子状态,如此用户就能依据量子状态的基本变化,对信息的状态加以详细判断,进而采取适合的防护措施,有效避免信息泄露带来的各种损失。

4.2 验证输入并对输入进行编码

安全问题的发生是受到劫持攻击,这种攻击可以运用 C 语言格式字符串进行,或者通过 Web 脚本中的语言进行跨站脚本攻击。若 Web 应用接收到了用户如入的信息,并将输入内容转发给某个功能,这样就非常容易被攻击。因而,要正确的验证并保证满足应用程序的要求。如:通过验证的方式,保证用户输入过程能够保证一定长度,并且不包括 HTML 字符,并且在使用中能够安全处理非法输入信息。在验证过程若有恶意字符,应对这些字符进行编码。

在此过程中要重视白名单的应用,白名单能验证相关参数的输入,并且通过实验证明,该方式利于过滤攻击以及未知的输入模式。相比较而言,黑名单的设置,更加能够有效的清理某些恶意的程序,还能用来进行临时过滤,并提高零日漏洞攻击的防范能力。

在检测到恶意的输入后,要保证能及时处理,并且要选择最佳的方式拒绝恶意输入。

如果客户端验证是作为第一层过滤而实施的,还应当测试其 JavaScript 情况 (JavaScript 在解析普通的表达式时与服务器的验证引擎略有不同,而且会在客户端生成似是而非的问题,并在服务器端产生“似非而是”的问题)。最后,测试者应当在关闭服务器端和客户端验证的情况下运行应用程序。这样做会揭示接受非法数据如何影响其它应用程序层,并会暴露漏洞。在对输入验证实施了集中化的架构中,测试还可以揭示是否在系统的其它点上需要其它的验证。必须确保验证不能被绕过。在客户端/服务器的设计中,服务器的验证是保护服务器的唯一验证。

4.3 避免将 ID 作为序列号

在软件开发设计过程,攻击者必然要超过现有限制,并且获得需要的数据信息。例如 API 的用户只被允许查看 ID 号为 1-100 的用户信息。该设计以 ID 为顺序,通过递增编号的方式,那么通过预测的方式,能够明确下一个用户的序列号为 101,这就给攻击者提供了逻辑漏洞,通过获取相关的权限容易获得信息。

示例:

包含潜在风险的Java代码

```
1. String sqlIdentifier = "select TESTING_SEQ.NEXTVAL from dual";
2. PreparedStatement pst = conn.prepareStatement(sqlIdentifier);
3. synchronized( this ){
4. ResultSet rs = pst.executeQuery();
5. if(rs.next())
6. long myId = rs.getLong(1);
```

安全的Java代码

```
1. // This example isfor Oracle
2. String sqlIdentifier = "select TESTING_SEQ.NEXTVAL from dual";
3. PreparedStatement pst = conn.prepareStatement(sqlIdentifier);
4. synchronized( this ){
5. ResultSet rs = pst.executeQuery();
6. if(rs.next())
7. long myId = rs.getLong(1) + UUID.randomUUID();
```

5 在信息安全背景下提升计算机软件开发水平的建议

5.1 全面提升软件开发人员的专业素养

在计算机软件开发工作的过程中,最为主要的就是软件开发的工作人员,在实施开发工作时要确保技术掌握的情况,比如要重视技术的先进性,并在工作的时候树立良好的职业道德准则,进而在技术上不断深入学习,推动技术的新进展。第一,工作的时候,负责软件开发的工作人员,必须要树立良好的创新性意识,利用技术的积极创新,还有计算机软件的有效优化,高质量地完成涉及到的工作内容。第二,随着信息技术的日益发展,软件开发公司的数量在不断增加着,有的技术人员因职业道德的不足,在行为上容易出现泄露软件的一些不良情况,促使软件开发的无法完全获得稳定。为此,作为软件开发的企业,必须要从多个方面,多个角度全方位的去思考,让行业的准入门槛不断加以提高,并且还要维护好软件市场环境的优质化,在过程中严格秉持着保密的基本原则,利用宏观调控政策让软件开发工作越来越处于安全稳定的状态。

5.2 重视计算机软件开发维护工作的作用

计算机软件开发工作的主要部分更多的是来自于维

护,利用科学化的维护体系,让软件的使用价值能够处于合理化状态,促使软件在应用过程中能够发挥出自身最大化的价值,为人们的日常生活和工作应用提供助力。对于软件开发工作人员而言,使用软件之后要实时跟踪软件的使用过程,若是在维护工作中遇到问题要先实施有效性的调整和科学化的修复。总体而言,从软件生态角度来分析,软件的维护变得越来越重要,同时也要重视配置方面管理,合理化控制好软件的配置,有效避免计算机应用时混乱问题的出现。

6 结束语

总之,通过实践分析,结合计算机软件开发工作开展实际,全面研究了安全技术计算机软件开发过程中有效应用的对策,作为新时期计算机软件开发技术人员,要提高安全认识,应在开发过程合理地运用安全技术方式,加强软件安全,有效地为用户提供更加高效安全的使用方式,从而提高计算机软件开发水平。

参考文献

- [1]周思远.安全技术计算机软件开发中的应用分析[J].电脑知识与技术,2020,16(28):72-73+76.
- [2]李晓琳.安全技术计算机软件开发中的价值和作用[J].信息与电脑(理论版),2020,32(18):88-89.
- [3]鲁佳炜.安全技术计算机软件开发中的应用[J].数字技术与应用,2020,38(05):181-182.
- [4]邓伟.安全技术计算机软件开发中的应用分析[J].中国新通信,2020,22(09):135.
- [5]李静.安全技术计算机软件开发中的应用[J].电脑知识与技术,2021(9):46-47.
- [6]黄妮妮.论安全技术计算机软件开发中的应用[J].数字通信世界,2020(2):99-100.
- [7]黄中琪.安全技术计算机软件开发中的应用研究[J].轻工科技,2021(5):88-89.
- [8]李喜梅,贺立强,贺军.安全技术计算机软件开发中的运用[J].电子技术与软件工程,2019(13):36.
- [9]刘俊芳.安全技术计算机软件开发中的应用分析[J].电脑知识与技术,2021,17(24):48-49+58.

作者简介:夏永贞(1982,1-),女,汉,河南新乡人,硕士学位,高级工程师职称,研究方向:软件工程系统控制。